



UNITED STATES PATENT AND TRADEMARK OFFICE

[Handwritten signature]

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHIED	33012/274/10	4721

7590 12/30/2003

CHARLES A JOHNSON
UNISYS CORPORATION
LAW DEPARTMENT M S 4773
2470 HIGHCREST ROAD
ROSEVILLE, MN 55113

EXAMINER

WASSUM, LUKE S

ART UNIT PAPER NUMBER

2177

DATE MAILED: 12/30/2003

13

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action

Application No.

09/448,154

Applicant(s)

GERMSCHIED ET AL.

Examiner

Luke S. Wassum

Art Unit

2177

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 08 December 2003 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE. Therefore, further action by the applicant is required to avoid abandonment of this application. A proper reply to a final rejection under 37 CFR 1.113 may only be either: (1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114.

PERIOD FOR REPLY [check either a) or b)]

- a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
- b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection. ONLY CHECK THIS BOX WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

1. ☐ A Notice of Appeal was filed on _____. Appellant's Brief must be filed within the period set forth in 37 CFR 1.192(a), or any extension thereof (37 CFR 1.191(d)), to avoid dismissal of the appeal.
2. ☐ The proposed amendment(s) will not be entered because:
- (a) ☐ they raise new issues that would require further consideration and/or search (see NOTE below);
 - (b) ☐ they raise the issue of new matter (see Note below);
 - (c) ☐ they are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
 - (d) ☐ they present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____

3. ☐ Applicant's reply has overcome the following rejection(s): _____.
4. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
5. ☒ The a) ☐ affidavit, b) ☐ exhibit, or c) ☒ request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
6. ☐ The affidavit or exhibit will NOT be considered because it is not directed SOLELY to issues which were newly raised by the Examiner in the final rejection.
7. ☒ For purposes of Appeal, the proposed amendment(s) a) ☐ will not be entered or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____


Claim(s) objected to: _____

Claim(s) rejected: 1-20.

Claim(s) withdrawn from consideration: _____

8. ☐ The drawing correction filed on _____ is a) ☐ approved or b) ☐ disapproved by the Examiner.
9. ☐ Note the attached Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____
10. ☒ Other: See Continuation Sheet


JOHN BREENE
SUPERVISORY PATENT EXAMINER


Luke S. Wassum
Art Unit 2177

Continuation of 5. does NOT place the application in condition for allowance because:

Regarding the objection to the specification, the examiner does not find the Applicants' arguments persuasive.

The objection to the specification stems from the fact that there are three different UserID/Passwords, which are treated differently, yet are not distinguished from each other in the specification. Thus, when referring to a UserID/Password, it is unclear to the reader which UserID/Password is being referred to.

Similarly, there seem to be two different User Validation Services which operate upon different data, yet are not distinguished from each other in the specification, which makes it unclear to the reader which User Validation Service is being referred to.

Furthermore, the Applicants' conclude that the examiner has misread the Applicants' claims, since "Nowhere in the claims do Applicants state that no "UserID/Password" need be transmitted over a network." (page 12, lines 1-3 of the Applicants' response). However, it is not the claims to which the examiner refers in citing the inconsistency in the specification, but in the specification itself. As previously stated by the examiner in the objection of record, the specification at page 7, lines 17-20 discloses the following: "This unique User Validation feature provides the capability for the browser to send information, which is then translated into a UserID/Password on the Cool ICE Web Application server. This bypasses the need to send a UserID/Password from browser to server, which enhances security." However, the specification goes on to detail how UserID/Password combinations are in fact transferred via the Internet to the server (as detailed in the objection of record). Clearly, there is some inconsistency in the specification, chiefly stemming from the fact that there are different UserID/Passwords, which are treated differently, but all referred to by the terms UserID/Password. This is the reason for the examiner's objection to the specification. This objection is maintained.

Regarding the claim rejections under 35 U.S.C. §112, first paragraph, the examiner does not find the Applicants' arguments persuasive.

As stated in the rejection of record, independent claims 1, 6, 11 and 16 are rendered non-enabled because they claim a system wherein "said database management system permits said user to access said at least one database from said user terminal at said particular site without transfer of said user identifier via said publically accessible digital data communication network." (representative language from claim 1). However, the specification states on replacement page 34, lines 9-12, that "...if a security profile has been identified for the service request, service handler 322 requests the user to provide a user-id via path 330, Cool ICE object 322, and world wide web path 312." This inconsistency between claims and specification renders the claims non-enabled.

Further regarding the 'special field' of claims 3, 7, 13 and 17, the said 'special field' is not referred to in any way in the detailed description and furthermore the apparent 'disclosure' to which the examiner was referred, message 2 of Figure 14, does not even refer to the special field by the same name, but by the term 'hidden field'. These facts render the claimed limitation non-enabled.

Regarding the generation of the site specific security profile, in spite of the fact that Figure 13 (and its corresponding description in the specification) provides no measure of enablement to an ordinary user, the examiner upon further investigation finds sufficient disclosure in the description of Figure 12, page 36 of the specification, as to enable the limitation.

Nonetheless, since all dependent claims inherit the deficiencies of the independent claims, the rejections of claims 1-20 under 35 U.S.C. §112 first paragraph is maintained.

Regarding the claim rejections under 35 U.S.C. §112, second paragraph, the examiner does not find the Applicants' arguments persuasive. For the reasons cited above regarding the inconsistencies of the specification, and in the rejection of record, the examiner maintains the rejections of claims 1-20 under 35 U.S.C. §112, second paragraph.

Regarding the Applicants' arguments that there would be no motivation to combine the system of Garrison with the other references, since Garrison teaches the encryption of the password, the examiner responds that encryption is one method of solving the problem of user identification and validation, and the method provided by the secondary references is a different method. The motivation to combine the references is sufficient to establish a prima facie case of obviousness.

Regarding the Applicants' argument that the di Vimercati reference does not say anything about *not* transferring a user identification, the examiner points out the teaching from page 88, second paragraph that "access to some federated data can be allowed to all users connected from site site1". This discloses the fact that the transmission of a user identification is not necessary for a user to be allowed access to data. Although the Applicants cite different methods of data security that are also taught by the reference, the above-cited passage is a sufficient teaching to anticipate the claimed limitation.

Regarding the Applicants' arguments that Yoshimoto fails to teach a security profile that is site specific, the examiner reiterates the rejection of record, and further quotes the reference at col. 1, line 67 through col. 2, line 6: "...comprising acquisition means for acquiring an identifier of a terminal which requests a service and an identifier of a user, decision means for uniquely deciding authority over the service request based upon the terminal identifier that have been acquired, and judging means for judging, using the authority that has been decided, whether or not to accept the service request." This teaches that the security profile is unique to a UserID/Terminal combination, and thus is specific to the site from which the request is being made.

Regarding the Applicants' arguments that the rejection of the 'signing on' limitation in view of Garrison is incorrect, the examiner respectfully responds that the disclosed client transmission of a password to the server in order to identify the user of the client as an authorized user would inherently require the identification of the user to the client system in the first place; without such action, there is no way for the client to know what user identification to transmit to the server.

Regarding the Applicants' arguments regarding the wording of the rejections, wherein the rejections of record state that Garrison teaches a security profile that 'corresponds to a site', and the later admission that Garrison does not teach a system with a site-specific security profile, the examiner apologizes for the miscommunication. In the relevant claim rejections, the language 'corresponding to said site' should not have been included in the portions taught by Garrison, since the teaching that the security profiles are site specific is in fact taught by Yoshimoto, as cited in the rejections of record.

Other arguments presented by the Applicants have been previously addressed, and the Applicants are referred to the Response to Arguments section of the previous Office action, Final Rejection, paper number 11.

Continuation of 10. Other:

The amendment to the specification is sufficient to resolve the drawing objections presented by the examiner in the Final Rejection.